DETAILED ACTION

1. This is in response to the amendment filed July 2, 2008. Claims 1, 6, 20, 23, 31, 45 and 50 have been amended. Claim 17 has been cancelled. Claims 1-16 and 18-51 are pending and have been considered below.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Bhavani S. Rayaprolu (Reg. 56,583) on September 10, 2008.

The application has been amended as follows:

Please amend claims 1, 6, 20, 23, 31, 32, 33, 41, 44, 50 and 51 as Follows:

Claim 1: (Currently amended) A machine-implemented system that facilitates spam detection comprising a processor executing:

a feature extraction component that receives an item and extracts a set of features associated with an origination of a message or part thereof and/or information that enables an intended recipient to contact or respond to the message;

a feature analysis component that analyzes a subset of the extracted features in connection with building and employing a plurality of feature-specific filters that are independently trained to mitigate undue influence of at least one feature type over another in the message, the subset of extracted features comprising of at least one of a Uniform Resource Locator (URL) and an Internet Protocol (IP) address, and the plurality of feature-specific filters comprising at least a first feature-specific filter; and

a machine learning component that determines last IP address external to the recipient's system *via* a machine learning technique to facilitate spam detection, the machine learning component employs MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record and determines whether the IP address is external or internal by verifying if the IP address is in a form characteristic to internal IP addresses and performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name.

Claim 6: (Currently amended) A machine-implemented system that facilitates spam detection comprising a processor executing:

a feature extraction component that receives an item and extracts a set of features associated with an origination of a message or part thereof and/or information that enables an intended recipient to contact or respond to the message;

at least one filter that is used when one of an Internet Protocol (IP) address of the message or at least some part of at least one of Uniform Resource Locator (URL) in the message is unknown; and

a machine learning component that determines last IP address external to the recipient's system via a machine learning technique to facilitate spam detection, the machine learning component employs MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record and determines whether the IP address is external or internal by verifying if the IP address is in a form characteristic to internal IP addresses and performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name.

Claim 20:(Currently amended) A machine-implemented system that facilitates spam detection comprising a processor executing:

a feature extraction component that receives an item and extracts a set of features associated with an origination of a message or part thereof and/or information that enables an intended recipient to contact or respond to the message;

at least one filter that is used when one of the Internet Protocol (IP) address of the message or at least some part of at least one of the Uniform Resource Locators (URLs) in the message is known; and

a machine learning component that determines last IP address external to the recipient's system *via* a machine learning technique to facilitate spam detection, the machine learning component employs MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record and determines whether the IP address is external or internal by verifying if the IP address is in a form characteristic to internal IP addresses and performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name.

Claim 23:(Currently amended) A machine learning method implemented on a machine that facilitates spam detection by optimizing an objective function of the form

OBJECTIVE(MAXSCORE(m1), MAXSCORE(m2), …, MAXSCORE(mk), w1…wn) where MAXSCORE(mk) = MAX(SCORE(IPk,1), SCORE(IPk,2), ..., SCORE(IPk,kl))

where mk = messages;

IPk,i represents the IP addresses ~~presence of some property(s)~~ of mk;

SCORE(IPk,i) = the sum of the weights of the ~~features of~~ IPk,i, and

wherein the machine learning method optimizes the weights associated with one feature at any given time and maximizes accuracy on a training data to facilitate improved detection of spam, the machine learning method employs MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record and determines whether the IP address is external or internal by verifying if the IP address is in a form characteristic to internal IP addresses and performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name and further determines last IP address external to a recipient's system to facilitate spam detection.

Claim 31:(Currently amended) A machine-implemented method that facilitates spam detection comprising:

providing a plurality of training data;

extracting a plurality of feature types from the training data, the feature types comprising at least one Internet Protocol (IP) address, at least one Uniform Resource Locator (URL) and text-based features; ~~and~~

training a plurality of feature-specific filters for the respective feature in an independent manner so that a first feature does not unduly influence a message score over a second feature type when determining whether a message is spam;

employing MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record;

~~concluding that~~ verifying if the IP address is in a form characteristic to internal IP addresses;

performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name; and

determining last IP address external to the recipient's system to facilitate spam detection.

Claim 32: (Currently amended) The method of claim ~~0~~ 31, the plurality of training data comprises messages.

Claim 33: (Currently amended) The method of claim ~~0~~ 31, the plurality of feature-specific filters comprises at least two of the following:

a known IP address filter;
an unknown IP address filter;
a known URL filter;
an unknown URL filter; and
a text-based filter.

Claim 41: (Currently amended) The method of claim ~~0~~ 31, further comprising combining message scores generated from at least two filters used to scan a new message to generate a total score that facilitates determining whether the message is spam.

Claim 44:(Currently amended) The method of claim ~~0~~ 31, further comprising quarantining messages that satisfy at least one criterion for a period of time until additional information about the message can be collected to update one or more feature-specific filters to facilitate determining whether the messages are spam.

Claim 50: (Currently amended) A machine-implemented method that facilitates spam detection comprising:

extracting data from a plurality of messages;

training at least one machine learning filter using at least a subset of the data, the training comprising employing a first smoothing for at least one of Internet Protocol (IP) address or Uniform Resource Locator (URL) features and at least a second smoothing for other non-IP address or non-URL features; ~~and~~

employing MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record;

verifying that the IP address is in a form characteristic to internal IP addresses;

performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name; and

determining last IP address external to the recipient's system to facilitate spam detection.

Claim 51: (Currently amended) The method of claim ~~0~~ 50, the smoothing differs in at least one of the following aspects:

the first smoothing comprises a different variance compared to the second smoothing with respect to a maximum entropy model; and

the first smoothing comprises a different value of weight decay compared to the second smoothing with respect to a Support Vector Machine (SVM) model.

Please cancel the following claims: 18 and 45-49.

Allowance

Claims 1, 6, 20, 23, 31, 32, 33, 41, 44, 50 and 51 have been amended and claims 18 and 45-49 have been cancelled. Support for the amendment can be found on Page 14, lines 15 – 26, Page 15, line 1 – Page 17, line 15 and Page 12, line 9 – 25 of Specification. Claims 1-16, 19-44 and 50-51 are allowed.

Examiner's Statement of Reason for allowance

The following is an examiner's statement of reasons for allowance:

1. The following is an examiner's statement of reasons for allowance:

Bandini et al discloses a system and method for filtering communication. An e-mail relay monitors incoming communication and compares attributes of the messages to data derived from SPAM messages, which is stored in a SPAM database. The e-mail relay restricts the delivery of the message based on the comparison such as by restricting the delivery of messages having attributes close to those of SPAM messages from the SPAM database.

Rothwell et discloses a system, method and computer program product are provided for detecting an unwanted message. First, an electronic mail message is received. Text in the electronic mail message is decomposed. Statistics associated with the text are gathered using a statistical analyzer. A neural network engine coupled to the statistical analyzer is taught to recognize unwanted messages based on statistical indicators. The statistical indicators are analyzed utilizing the neural network engine for determining whether the electronic mail message is an unwanted message.

Huang disclose a system and method of dynamic routing is provided. When a connection cannot be built, execute the follows. (a) A sending-host transports messages to destination-host. If connection built, the method ends, otherwise go to step (b). (b) Find a series of routers, and put IP-addresses of routers into a list. (c) Judge whether list includes at least one IP-address; if yes, go to step (d), otherwise step (i). (d) A pointer points to the last. (e) Find a domain of IP-address pointed. (f) If a message-routing-in-charge host is found, go to step (g), otherwise step (h). (g) The sending-host transports messages to message-routing-in-charge host, and go to step (a). (h) If IP-address pointed is the first one, go to step (i), otherwise step (j). (i) The sending-host keeps messages for a period, and go to step (a). (j) Move pointer to point to the previous, and go to step (e).

The prior art of reference taken alone or in combination do not teach or render obvious the limitations as recited in independent claims 1, 6, 20, 23, 31 AND 50. The claimed subject matter relates to systems and methods that facilitate detecting spam messages in part by scanning messages using a filter trained on IP address or URL features and another filter independently trained on text-related features and/or other features extractable from a message. In particular, independent claims 1, 6, 20, 23, 31, 45 and 50 recites ***a machine learning component that determines last IP address external to the recipient's system via a machine learning technique to facilitate spam detection, the machine learning component employs MX records to determine a true source***

of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record and determines whether the IP address is external or internal by concluding that the IP address is in a form characteristic to internal IP addresses and performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136